

What is claimed is:

1                   1.       A method of controlling security of data in a storage system having  
2 a local disk system and a remote disk system comprising:

3                   in the local disk system:

4                   when a write of data is to be made to the local disk system  
5 retrieving a previously stored encryption key;

6                   encrypting the data;

7                   transferring the data to the remote disk system; then

8                   in the remote disk system:

9                   determining whether the data is to be stored in an encrypted form;

10                  determining an address for storage of the data;

11                  if the data is to be stored in a decrypted form, decrypting the data;

12                  writing the data in the remote disk system; and

13                  notifying the local disk system that the step of writing the data is

14 complete.

1                   2.       A method as in claim 1 further comprising a step of maintaining an  
2 encryption control table on the local disk system, the encryption control table including a  
3 list of encryption keys for selected volumes of the local and the remote disk system.

1                   3.       A method as in claim 2 wherein the list of encryption keys further  
2 includes information relating to the use and non-use of encryption on the local disk  
3 system.

1                   4.       A method as in claim 2 wherein the list of encryption keys further  
2 includes information relating to the use and non-use of encryption on the remote disk  
3 system.

1                   5.       A method as in claim 3 wherein the encryption key is applicable to  
2 less than all of the storage on the local disk system.

1                   6.       A method as in claim 4 wherein the encryption key is applicable to  
2 less than all of the storage on the remote disk system.

09618202 "071800  
000720" 20070926

1           7.     A method as in claim 3 wherein the encryption key is applicable to  
2 at least one disk on the local disk system.

1           8.     A method as in claim 7 wherein the encryption key is applicable to  
2 at least one disk on the remote disk system.

1           9.     A method for changing an encryption key while operating a storage  
2 system having a local disk system and a remote disk system comprising:  
3                   storing an encryption key in a memory in the local disk system;  
4                   transmitting the encryption key to the remote disk system and  
5 storing it in a memory there;  
6                   in the local disk system determining a boundary for use of the  
7 encryption key;  
8                   in both the local and the remote disk system, determining a  
9 relationship of present operations to the boundary;  
10                  in both the local and the remote disk system waiting for the  
11 boundary, and then changing the encryption key for data stored thereafter.

1           10.    A method as in claim 9 wherein operations before the boundary are  
2 performed using a first encryption key and operations after the boundary are performed  
3 using a second encryption key.

1           11.    A method as in claim 9 wherein the boundary is defined by  
2 counting input/output operations and using the count to define the boundary.

1           12.    A method for changing an encryption key while operating a storage  
2 system having a local disk system and a remote disk system comprising:  
3                   storing an encryption key in a memory in the local disk system;  
4                   transmitting the encryption key to the remote disk system and  
5 storing it in a memory there;  
6                   splitting the local disk system from the remote disk system to allow  
7 them to operate independently;  
8                   using a new encryption key to begin storing data in the local disk  
9 system; and  
10                  resynchronize the local disk system and the remote disk system.

13. A method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

- maintaining a control table in each of the local disk system and the remote disk system;
- determining a boundary in the local disk system where encryption is to be switched to an opposite state;
- determining a corresponding boundary in the remote disk system;
- in both the local and the remote disk system, determining a relationship of present operations to the boundary;
- in both the local and the remote disk system waiting for the boundary, and then changing the switching the encryption to the opposite state.

14. A method as in claim 13 wherein operations before the boundary are either encrypted or not encrypted, and operations performed after the boundary are either not encrypted or encrypted oppositely to those operations performed before the boundary.

15. A method as in claim 14 wherein the boundary is defined by counting input/output operations and using the count to define the boundary.

16. A method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

- storing an encryption key in a memory in the local disk system;
- transmitting the encryption key to the remote disk system and storing it in a memory there;
- splitting the local disk system from the remote disk system to allow them to operate independently;
- switching encryption to an opposite state from a previous state; and
- re-synchronizing the local disk system and the remote disk system.

17. A storage system comprising:  
a local system including a plurality of volumes of media for storing data;  
a first computer program operating on the local system to determine  
whether encryption is to be employed in storage of data on the local system, and if so,

5 retrieving an encryption key from storage and using the key to encrypt the data to be  
6 stored;

7 a communications link coupling the local system to the remote system; and  
8 a second computer program operating on the remote system to store the  
9 data in either encrypted form or unencrypted form based and storing the data in that form  
10 in the remote system, and notifying the local disk system that the data has been stored.

1 18. A system as in claim 17 further comprising an encryption control  
2 table stored on the local disk system, the encryption control table including a list of  
3 encryption keys for selected volumes of the local system and the remote system.

1 19. A system as in claim 18 wherein the list of encryption keys further  
2 includes information relating to the use and non-use of encryption on the local system.

1 20. A system as in claim 19 wherein the list of encryption keys further  
2 includes information relating to the use and non-use of encryption on the remote system.

1 21. A system as in claim 20 wherein the encryption key is applicable to  
2 less than all of the storage on the local system.

1 22. A system as in claim 21 wherein the encryption key is applicable to  
2 less than all of the storage on the remote system.

1 23. A storage system having a local system and a remote system, and  
2 having changeable encryption keys, comprising:

3 a local memory which stores an encryption key in the local system;

4 a communications link connecting the local system to the remote system  
5 for transmitting the encryption key to the remote disk system;

6 a remote memory which stores the encryption key in the remote system;

7 a first computer program in the local system which determines a boundary  
8 for use of the encryption key; and

9 in both the local and the remote disk system, a second computer program  
10 for determining a relationship of present operations to the boundary, and changing the  
11 encryption key for operations occurring after the boundary.

03613202 071300

1                   24.     A system as in claim 23 wherein the second computer program  
2 counts input/output operations to define the boundary.

1                   25.     A storage system having a local system and a remote system, and  
2 having changeable encryption keys, comprising:  
3                   a local memory which stores an encryption key in the local system;  
4                   a communications link connecting the local system to the remote system  
5 for transmitting the encryption key to the remote disk system;  
6                   a remote memory which stores the encryption key in the remote system;  
7                   a first computer program in the local system which determines a boundary  
8 for use of the encryption key and splitting of the local system from the remote system;  
9                   in both the local and the remote disk system, a second computer program  
10 for determining a relationship of present operations to the boundary, and splitting the  
11 local system from the remote system at the boundary;  
12                  a third computer program for re-synchronizing the local system and the  
13 remote system.

1                   26.     A system for controlling encryption in a storage system having a  
2 local system and a remote system comprising:  
3                   a local memory storing an encryption key in the local system;  
4                   a communications link for transmitting the encryption key to the remote  
5 disk system and storing it in a remote memory there;  
6                   a first computer program for splitting the local system from the remote  
7 system to allow them to operate independently;  
8                   a switch for changing encryption to an opposite state from a previous state;  
9 and  
10                  a second computer program for re-synchronizing the local system and the  
11 remote system.

1                   27.     A method of controlling security of data in a storage system having  
2 a local disk system and a remote disk system comprising:  
3                   in the local disk system:  
4                   assigning a key to a first portion of the local disk system;

5                    encrypting the data stored in the first portion of the local disk  
6 system;  
7                    transferring the encrypted data to the remote disk system; then  
8                    in the remote disk system:  
9                    decrypting the data using the assigned key; and  
10                    writing the decrypted data into a second portion of the remote disk  
11 system.

1                    28.     A method as in claim 27 wherein the first portion comprises at least  
2 a volume of the local storage system and the second portion comprises at least a volume  
3 of the remote disk system.

1                    29.     A method as in claim 28 wherein the first portion comprises a  
2 group of volumes of the local storage system, and the second portion comprises a group  
3 of volumes of the remote storage system.

1                    30.     A storage system comprising:  
2                    a local system including a plurality of volumes of media for storing data;  
3                    a remote system including a plurality of volumes of media also for storing  
4 data;  
5                    a first computer program operating on the local system to retrieve selected  
6 data from storage on the local system, and encrypt that selected data using an encryption  
7 key;  
8                    a communications link coupling the local system to the remote system for  
9 transmitting the encrypted selected data to the remote system; and  
10                    a second computer program operating on the remote system to decrypt the  
11 selected data received from the communications link and store that selected data in  
12 unencrypted form in the remote system.

1                    31.     A system as in claim 30 further comprising an encryption control  
2 table stored on the local disk system, the encryption control table including a list of  
3 encryption keys for selected volumes of the local system and the remote system.

09040202.07.1000